UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,369	03/30/2004	Douglas S. Ransom	6270/139	4719

46260 7590 07/18/2008

BRINKS HOFER GILSON & LIONE/PML
PO BOX 10395
CHICAGO, IL 60610

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,369	RANSOM ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 04/29/2008. Claims 1-41 are pending and have been considered as follows.

Examiner Note

In light of the applicant's amendments, the examiner hereby withdraws his previous Claim Objections with respect to Claims 1, 5-24, 29-32, & 41.

Claim Objections

1. Claims 1, 32, & 41 are objected to because of the following informalities:

- Claim 1 line 19 recites the term "when" which should be "…if…";
- Claim 32 line 9 recites the term "when" which should be "…if…";
- Claim 41 line 8 recites the term "when" which should be "…if…";

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-4, 14, 16, 21, 22, 24-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Selph et al. (US-4804957-A).

Claim 1:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network comprising,

- "an energy distribution system interface configured to couple said energy management device with at least a portion of said energy distribution system" (i.e. "The electric utility service enters through service drop cable 28, which may include one or more hot conductors and neutral. The electric utility service enters riser conduit 24, passes through socket 22 and enters the building structure through entrance cable 30") [column 5 12-16];
- "a network interface configured to couple said energy management device with said network for transmitting outbound communications to said network" (i.e. "Meter interface unit 36 is coupled to meter 20 and provides communication between the meter and the commercial telephone network") [column 5 lines 35-37];

- "said outbound communications comprising energy management data" (i.e. "The electrical readout signals from meters 38 and 40 are delivered to the utility meter 20 of the invention through connection lines 42") [column 5 lines 49-55];
- "a processor coupled with said network interface and said energy distribution system interface, configured to generate said energy management data" [Fig 6A illustrates a processor interfaced with various components associated with the meter];
- "an enclosure which surrounds said energy management device and protects said energy management device from tampering" (i.e. "The invention is housed in an enclosure which prevents physical tampering with the electronic circuitry") [column 3 lines 35-36];
- "a tamper prevention seal coupled with said enclosure, which detects unauthorized access to said enclosure" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor") [column 3 lines 39-40];
- "a seal tamper detection unit coupled with said processor and said tamper prevention seal and configured to detect when said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44];

- "wherein said energy management device is configured to take at least one internal protective action when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "If the processor becomes inactive or locks up due to tampering or spurious power line signals, the watchdog circuit detects this condition and restarts the processors control routine") [column3 lines 48-51].

Claim 2:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "said tamper seal comprises a revenue seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 3:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "said tamper seal comprises a metering point id seal" (i.e. "a tamper detection device") [column 3 lines 39-40].

Claim 4:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "a memory coupled with said processor" (i.e. "A memory, such as a random access memory, is coupled to the processor for storing the digital information") [column 2 lines 62-64];
- "said memory configured to store confidential data" (i.e. "A memory, such as a random access memory, is coupled to the processor for storing the digital information") [column 2 lines 62-64].

Claim 14:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "said processor is further configured to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 16:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "a memory coupled with said processor and configured to store at least one device setting" (i.e. "During normal operation, microprocessor 138 executes a programmed set of instructions (contained within internal memory or optionally within program memory 158)") [column 10 lines 18-21];
- "wherein said processor is further configured to send a message warning that said device setting has been changed through said network interface when said at least one device setting has been changed after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 21:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "said processor is further configured to set off a security alarm when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 22:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "a display coupled with said processor and configured to visually display text" (i.e. "A display, such as an LED or liquid crystal 7 segment display, is responsive to the processor and provides a visual indication of the digital information provided by the processor") [column 2 lines 67-68];
- "wherein said processor is further configured to place a warning message on said display when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" (i.e. "to provide an alarm event indication in response to a predetermined fault condition") [column 3 lines 17-18].

Claim 24:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "said seal tamper detection unit further comprises a sensor configured to detect that said tamper prevention seal is broken" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor") [column 3 lines 39-40].

Claim 25:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 24 above, further comprising,

- "said sensor comprises a limit switch" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 26:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 24 above, further comprising,

- "said sensor comprises a proximity sensor" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 27:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 26 above, further comprising,

- "said proximity sensor comprises at least one of a pin, an optical proximity sensor, an optical motion detector, a grounding tab, an ultrasonic sensor, an electro-magnetic sensor and a gyroscope" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 28:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 24 above, further comprising,

- "said sensor comprises at least one of a camera and a video camera" (i.e. "In addition to sensing electric power consumption, the invention is also capable of receiving, arbitrating and processing signals from other utility sensors including water flow sensors, gas flow sensors, and other utility metering devices. Further, the invention can also sense and report emergencies such as fire or intrusion") [column 2 lines 52-58].

Claim 29:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "an energy storage device coupled with said seal tamper detection unit and configured to provide power to said seal tamper detection unit in power outage situations" (i.e. "a backup power source comprising a storage battery and a low battery detection circuit") [column 3 lines 30-32].

Claim 30:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "said processor is further configured to perform at least one energy management function on said at least a portion of said energy distribution network via said energy distribution system interface" (i.e. "As will be explained in detail below, meter 20 measures the

magnetic field generated by the incoming electric current. Entrance cable 30 enters building structure 26 for attachment to a distribution panel 27 with fuses or circuit breakers in the usual fashion") [column 5 16-21];

- "said processor further operative to generate said energy management data as a function of said energy management function" (i.e. "As will be explained in detail below, meter 20 measures the magnetic field generated by the incoming electric current. Entrance cable 30 enters building structure 26 for attachment to a distribution panel 27 with fuses or circuit breakers in the usual fashion") [column 5 16-21].

Claim 31:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "an enclosure defining an interior and an exterior and configured to enclose said energy management device within said interior and to limit access to said energy management device" (i.e. "The invention is housed in an enclosure which prevents physical tampering with the electronic circuitry") [column 3 lines 35-36];
- "said tamper prevention seal is coupled with said enclosure and configured to deter unauthorized access to said interior of said enclosure and indicate any such access" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-40].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 5-13, 15, 18, 23, 32-39, & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Selph et al. (US-4804957-A) in view of Shear et al. (US-6157721-A).

Claim 5:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 4 above, but they do not disclose,

- "said processor is further configured to delete said confidential data from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest the discarding of information to protect against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to delete said confidential data from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. for the purposes of protecting against unauthorized access.

Claim 6:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 4 above, but they do not disclose,

- "said processor is further configured to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 7:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 4 above, but they do not disclose,

- "said confidential data comprises a private key configured to sign said energy management data," although Shear et al. do suggest the usage of asymmetric key cryptography and message digests, as recited below;

however, Shear et al. do disclose,

- "Message digest 116 may then be encrypted using asymmetric key cryptography" [column 13 lines 30-31];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said confidential data comprises a private key configured to sign said energy management data," in the invention as disclosed by Selph et al. since the usage of asymmetric cryptography and message digests are common methodologies for protecting content.

Claim 8:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 7 above, but Selph et al. do not disclose,

- "said processor is further configured to delete said private key from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to delete said private key from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 9:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 7 above, their combination further comprising,

- "said processor is further configured to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred, and to sign said message with said private key" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 10:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 4 above, but they do not disclose,

- "said confidential data comprises a certificate configured to sign said energy management data," although Shear et al. do suggest using digital signatures, as recited below;

however, Shear et al. do disclose,

- "Protected processing environments 108 can use this digital "seal of approval" 106 (which may comprise one or more "digital signatures") to distinguish between authorized and unauthorized load modules 54" [column 9 lines 52-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said confidential data comprises a certificate configured to sign said energy management data," in the invention as disclosed by Selph et al. since digital signatures are a common form of certification to distinguish between authorized and unauthorized information.

Claim 11:

Selph et al. and Shear et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 10 above, but Selph et al. do not disclose,

- "said processor is further configured to delete said certificate from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to delete said certificate from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 12:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, but they do not disclose,

- "said processor is further configured to prevent said transmitting of said energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to prevent said transmitting of said energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 13:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, but they do not disclose,

- "said processor is further configured to prevent said transmitting of signed energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to prevent said transmitting of signed energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 15:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, further comprising,

- "a memory coupled with said processor and configured to store at least one device setting" (i.e. "During normal operation, microprocessor 138 executes a programmed set of instructions (contained within internal memory or optionally within program memory 158)") [column 10 lines 18-21];

but they do not disclose,

- "wherein said processor is further configured to prevent changes to said at least one device setting when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein said processor is further configured to prevent changes to said at least one device setting when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 18:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, but they do not disclose,

- "said processor is further configured to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 23:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, but they do not disclose,

- "said processor is further configured to mark said energy management data as unreliable when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to mark said energy management data as unreliable when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest preventing access.

Claim 32:

Selph et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network comprising,

- "protecting said integrity of said data by said energy management device in response to said detecting" (i.e. "The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 41-44];

- "said energy management device acting to internally protect said data as generated, stored, or transmitted thereby" (i.e. "If the processor becomes inactive or locks up due to tampering or spurious power line signals, the watchdog circuit detects this condition and restarts the processors control routine") [column3 lines 48-51];

but they do not disclose,

- "generating said data based on said at least one power parameter," although Shear et al. do suggest at least one or more computer instructions, as recited below;
- "said data being characterized by an integrity," although Shear et al. do suggest a sequence of instructions or steps that bring about a certain result, as recited below;
- "detecting when said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest determining authorized or unauthorized accesses, as recited below;

however, Shear et al. do disclose,

- "the load module preferably comprises one or more computer instructions and/or data elements used to assist, allow, prohibit, direct, control or facilitate at least one task performed at least in part by an electronic appliance such as a computer…load module 54 may comprise all or part of an executable computer program and/or associated data ("executable"), and may constitute a sequence of instructions or steps that bring about a certain result within a computer or other computation element" [column 8 lines 21-28];
- "the protected processing environment 108 can distinguish between authorized and unauthorized load modules 54 by examining the load module to see whether it bears the seal of verifying authority 100" [column 9 lines 58-61];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "generating said data based on said at least one power parameter" and "said data being characterized by an integrity" and "detecting when said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. for the purposes of determining authorized or unauthorized accesses.

Claim 33:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, their combination further comprising,

- "said energy management device stores confidential data" (i.e. "A memory, such as a random access memory, is coupled to the processor for storing the digital information") [column 2 lines 62-64];

but Selph et al. do not disclose,

- "c) further comprises deleting said confidential data," although Shear et al. do suggest discarding information, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "c) further comprises deleting said confidential data," in the invention as disclosed by Selph et al. for the purposes of securely protecting itself against unauthorized access.

Claim 34:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, their combination further comprising,

- "said energy management device stores confidential data" (i.e. "A memory, such as a random access memory, is coupled to the processor for storing the digital information") [column 2 lines 62-64];

but Selph et al. do not disclose,

- "c) further comprises preventing access to said confidential data," although Shear et al. do suggest protecting against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "c) further comprises preventing access to said confidential data," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest prevention of unauthorized access.

Claim 35:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, but Selph et al. do not disclose,

- "c) further comprises preventing transmission of said data," although Shear et al. do suggest protection against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "c) further comprises preventing transmission of said data," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest prevention of unauthorized access.

Claim 36:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, but Selph et al. do not disclose,

- "c) further comprises preventing signing of said data," although Shear et al. do suggest protection against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "c) further comprises preventing signing of said data," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest prevention of unauthorized access.

Claim 37:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, their combination further comprising,

- "c) further comprises generating a warning message" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 38:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, their combination further comprising,

- "said energy management device stores device settings" (i.e. "During normal operation, microprocessor 138 executes a programmed set of instructions (contained within internal memory or optionally within program memory 158)") [column 10 lines 18-21];

but, Selph et al. do not disclose,

- "c) further comprises preventing changes to said device settings," although Shear et al. do suggest protection against unauthorized access, as recited below;

however, Shear et al. do disclose,

- "Protected processing environment 108 discards and does not use any load module 54 that does not bear this seal 106. In this way, protected processing environment 108 securely protects itself against unauthorized load modules 54 such as, for example, the defective load module 54d made by disreputable load module provider 64" [column 9 lines 64-66];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "c) further comprises preventing changes to said device settings," in the invention as disclosed by Selph et al. since protection against unauthorized access would suggest prevention of unauthorized access.

Claim 39:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, their combination further comprising,

- "said energy management device stores device settings" (i.e. "During normal operation, microprocessor 138 executes a programmed set of instructions (contained within internal memory or optionally within program memory 158)") [column 10 lines 18-21];
- "c) further comprises generating a warning message if said device settings are changed" (i.e. "The enclosure includes a tamper detection device associated with the housing and coupled to the processor. The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 39-44].

Claim 41:

Selph et al. disclose a system for protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network comprising,

- "means for taking action to protect said integrity of said data by said energy management device in response to said means for detecting" (i.e. "The tamper detection device transmits a tamper alert signal which the processor can output through the communication means to the home office or monitoring substation") [column 3 lines 41-44];
- "said energy management device acting to internally protect said data as generated, stored or transmitted thereby" (i.e. "If the processor becomes inactive or locks up due to tampering or spurious power line signals, the watchdog circuit detects this condition and restarts the processors control routine") [column3 lines 48-51];

but, Selph et al. do not disclose,

- "means for generating said data based on said at least one power parameter," although Shear et al. do suggest at least one or more computer instructions, as recited below;
- "said data characterized by an integrity," although Shear et al. do suggest a sequence of instructions or steps that bring about a certain result, as recited below;
- "means for detecting when said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest determining authorized or unauthorized accesses, as recited below;

however, Shear et al. do disclose,

- "the load module preferably comprises one or more computer instructions and/or data elements used to assist, allow, prohibit, direct, control or facilitate at least one task performed at least in part by an electronic appliance such as a computer…load module 54

may comprise all or part of an executable computer program and/or associated data ("executable"), and may constitute a sequence of instructions or steps that bring about a certain result within a computer or other computation element" [column 8 lines 21-28];

- "the protected processing environment 108 can distinguish between authorized and unauthorized load modules 54 by examining the load module to see whether it bears the seal of verifying authority 100" [column 9 lines 58-61];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "means for generating said data based on said at least one power parameter" and "said data characterized by an integrity" and "means for detecting when said tamper prevention seal indicates that unauthorized access has occurred," in the invention as disclosed by Selph et al. for the purposes of determining authorized or unauthorized accesses.

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Selph et al. (US-4804957-A) in view of Gilgenbach et al. (US-6801865-B2).

Claim 17:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, but they do not disclose,

- "a memory coupled with said processor and configured to store a device configuration," although Gilgenbach et al. do suggest a memory storing configurations, as recited below;
- "said device configuration having at least one first device setting having a first value," although Gilgenbach et al. do suggest that the meter is programmed to operate as configured, as recited below;

- "said processor being configured to generate said energy management data based on said first value and to determine that said at least one first device setting has been modified to at least one second value after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Gilgenbach et al. do suggest comparing configurations, as recited below;
- "said processor being further configured to generate said energy management data based on said first value and generate alternate energy management data based on said at least one second value in response to said modification," although Gilgenbach et al. do suggest sending a request to replace the configuration, as recited below;

however, Gilgenbach et al. do disclose,

- "in order to restore default configuration parameter(s) stored in a memory of the meter 12" [column 14 lines 8-9];
- "Each meter 12 preferably operates according to one or more internal settings or configuration parameters" [column 5 lines 51-52];
- "The communications application software 50 then preferably compares (at 106) one or more of the actual configuration parameters to one or more of the corresponding default configuration parameters for the meter 12" [column 13 lines 4-7];
- "when a tamper event is indicated, the communications application software 50 can preferably either recall or again download (at 114) the default configuration parameter(s) for the meter 12 from the database 46" [column 13 lines 64-67];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a memory coupled with said processor and configured to store a device configuration" and "said device configuration having at least one first device setting having a first value" and "said processor being configured to generate said energy management data based on said first value and to determine that said at least one first device setting has been modified to at least one second value after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" and "said processor being further configured to generate said energy management data based on said first value and generate alternate energy management data based on said at least one second value in response to said modification," in the invention as disclosed by Selph et al. for the purposes of protecting the meter configuration.

7. Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Selph et al. (US-4804957-A) in view of Shear et al. (US-6157721-A) and in further view of Gilgenbach et al. (US-6801865-B2).

Claim 40:

Selph et al. and Shear et al. disclose a method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal configured to deter unauthorized access to said energy management device and indicate any such access, wherein said energy management device senses at least one power parameter from a power distribution network, as in Claim 32 above, but their combination do not disclose,

- "d) detecting that said at least one first device setting has been modified to have at least one second value," although Shear et al. do suggest comparing configurations, as recited below;
- "c) further comprises generating alternate data based on said at least one second value in addition to said data," although Shear et al. do suggest sending a request to replace the configuration, as recited below;

however, Gilgenbach et al. do disclose,

- "The communications application software 50 then preferably compares (at 106) one or more of the actual configuration parameters to one or more of the corresponding default configuration parameters for the meter 12" [column 13 lines 4-7];
- "when a tamper event is indicated, the communications application software 50 can preferably either recall or again download (at 114) the default configuration parameter(s) for the meter 12 from the database 46" [column 13 lines 64-67];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "d) detecting that said at least one first device setting has been modified to have at least one second value" and "c) further comprises generating alternate data based on said at least one second value in addition to said data," in the invention as disclosed by Selph et al. and Shear et al. for the purposes of protecting the meter configuration.

8. Claims 19 & 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Selph et al. (US-4804957-A) in view of Shear et al. (US-6157721-A) and in further view of Schneier et al. (US-5978475-A).

Claims 19 & 20:

Selph et al. disclose an energy management device used in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, as in Claim 1 above, but they do not disclose,

- "said processor is further configured to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred," although Shear et al. do suggest the common usage of audit logs, as recited below;
- "said processor is further configured to at least one of hash and encrypt said audit log," although Schneier et al. do suggest the usage of message digests for resistance against attacks, as recited below;

however, Shear et al. do disclose,

- "Audit logs have long been used to keep permanent records of critical events. The basic idea is that the audit log can be used at some future date to reconstruct events that happened in the past. This reconstruction might be required for legal purposes (to determine who did what when), for accounting purposes, or to reconstruct things after a disaster: errors, loss of data, deliberate sabotage, etc" [column 1 lines 1-10];

whereas, Schneier et al. do disclose,

- "In the FIG. 5 process, load module 54 (along with specifications 110 if desired) is processed to yield a "message digest" 116 using a conventional one-way hash function selected to provide an appropriate resistance to algorithmic attack" [column 13 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said processor is further configured to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred" and "said processor is further configured to at least one of hash and encrypt said audit log," in the invention as disclosed by Selph et al. for the purposes of keeping secure records.

Response to Arguments

9. Applicant's arguments filed 04/29/2008 have been fully considered but they are not persuasive.

- The applicant's remarks, "Selph neither teaches nor discloses an "energy management device [I configured to take at least one internal protective action when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred"" and "Shear does not teach or suggest any of the internal protective actions taken by applicants' energy management device and claimed in dependent claims 5- 13, 15, 18, 23" and "neither Selph nor Shear disclose "protecting said integrity of said data by said energy management device in response to said detecting, said energy management device acting to internally protect said data as generated, stored, or

transmitted thereby"" and "neither Selph nor Shear teach or suggest "means for taking action to protect said integrity of said data by said energy management device in response to said means for detecting, said energy management device acting to internally protect said data as generated, stored or transmitted thereby"," have been carefully considered but are non-persuasive at this point in time;

- The examiner notes that the current claim language of the applicant's independent claims only recite for "internal protection/internal protective action" that is taken upon a detection of tampering, and does not recite the explicit limitations found in their dependents. Thus, Selph et al.'s disclosure of "If the processor becomes inactive or locks up due to tampering or spurious power line signals, the watchdog circuit detects this condition and restarts the processors control routine" [column3 lines 48-51] would read on the applicant's current independent claim limitations with respect to the "internal protection/internal protective action".
- The examiner admits that Selph et al. alone do not provide explicit and detailed disclosure for the dependent limitations further limiting the scope of the "internal protection/internal protective action" as found on pages 12-13 of the applicant's remarks, however, reliance was made in view of Shear et al. for providing at the very least suggestion for the claimed types of actions/counter measures that are taken to protect a secure computing environment/system in the event of tampering or to prevent tampering.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
07/17/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136